A Study on Cloud Computing Security with Encryption and Decryption Technique

G. Naga Srikanth
Lecturer
Aditya Degree College
Kakinada
E.G.Dt., A.P.,

Dr. G. Naga Satish
Asssociate Professor
Aditya Engineering College
Surampalem
E.G.Dt., A.P.,

Dr. P. Suresh Varma
Professor-CSE
Adikavi Nannaya University,
Rajahmudry
E.G.Dt., A.P.,

I. R. Krishnam Raju
Research Scholar
Adikavi Nannaya
University, RJY
E.G.Dt.,A.P.,

***Abstract*— Cloud Computing has been developed to provide services to the users and individuals by reducing the expenses. Cloud computing improves performance of the organization by make use of minimum resources and management support, with a shared network, valuable resources bandwidth, software's and hardware's in a cost of use manner and limited service provider communications. Systematize cloud computing in an enterprise infrastructure bring significant security concerns. Successful implementation of cloud computing in an enterprise requires proper planning and understanding of emerging risks, threats, vulnerabilities, and possible countermeasures. Cloud security is becoming a key differentiator and competitive edge between cloud providers. In This paper we discuss the various types of cloud, security issues at cloud and network level and an encryption algorithm.**

Keywords: Cloud Computing, Threats, Vulnerabilities

I. INTRODUCTION

Cloud computing provides the facility to access unlimited infrastructure to share business needs. Cloud computing is can be defined basically as virtualization of the Technology and providing them as service to the end user [2]. The main aspects of cloud computing are

- Virtualization
- Utility Computing
- Scalability

Virtualization means separating the Technology and Data from the Physical hardware. Virtualization is the heart of Cloud Computing as it completely depends on it. Scalability feature provides the flexibility to the cloud user and the provider. It makes the cloud to with stand any changes with out affecting the performance of the entire system. Utility computing is the one where the software, Infrastructure and platform are provided to cloud computing users as service. Security control measures in cloud are similar to ones in the traditional IT environment. Due to the openness of the cloud, cloud computing is impacting on the security field [1]. Due to dynamic scalability, service abstraction, and location transparency features of cloud computing models, all kinds of applications and data on the cloud platform have no fixed infrastructure and security boundaries. It is difficult to isolate a particular physical resource that has a threat or has been compromised. As the cloud platform has to deal with massive information storage and to deliver a fast access, cloud security measures have to meet the need of massive information processing.

A. Characteristics

Cloud computing has a wide range of characteristics some of which are as follows:

- **Shared Infrastructure:** cloud environment uses an effective software model that allows sharing of physical services, storage and networking capabilities among users. The cloud infrastructure is to find out most of the available infrastructure across multiple users.
- **Network Access:** Cloud services are accessed over a network from a wide range of devices such as PCs, laptops, and mobile devices by using standards based APIs.
- **Handle Metering:** Cloud service providers store information of their clients for managing and optimizing the service and to provide reporting and billing information. Due to this, customers are payable for services according to how much they have actually used during the billing period.

This paper describes the network and security issues in the cloud computing. This paper is organized as follows: Section II gives brief description about the cloud service models. Section III describes the types of clouds. Section IV describes the Data Security Issues. Section V describes the Network level security. Section VI describes the encryption algorithm with experimental results.

II. CLOUD SERVICE MODELS

Cloud Computing provides three ways of service.

- Such as Software-as-a-Service (SaaS)
- Platform-as-a-Service (PaaS)
- Storage-as-a- Service and Infastructure-as-a-Service (IaaS).

A. Software as a Service (SaaS)

It is sometimes referred to as Service or Application Clouds are offering execution of specific business functions and business development that are provided with specific cloud capabilities, i.e. they provide applications or services using a cloud infrastructure or platform, rather than providing cloud features themselves.

Examples: Google Docs, Salesforce CRM, SAP Business by Design.

Figure 1 Software as Service

B. Platform as a Service (PaaS)

Provides computational possessions via a platform upon which applications and services can be developed and hosted. PaaS typically makes use of dedicated APIs to control the behavior of a server hosting engine which executes and replicates the execution according to user requests (e.g. access rate). As each provider exposes his / her own API according to the respective key capabilities, applications developed for one specific cloud provider cannot be moved to another cloud host – there are however attempts to extend generic programming models with cloud capabilities.

Examples: Force.com, Google App Engine, Windows Azure (Platform).

Figure 2 Platform as Service

C. Infrastructure as a Service

IaaS provides CPU, Memory, Storage, networking and security as a package. The IaaS also referred to as Resource Clouds, provide resources as services to the user. IaaS (Infrastructure as a Service) offers additional potential over a simple compute service.
Examples: Amazon S3, SQL Azure.

Figure 3 Software as Service

III. TYPES OF CLOUDS

There are four types of cloud computing models: private cloud, public cloud, hybrid cloud and community cloud.

A. Public Cloud

It is for the general public where resources, web applications, web services are provided over the internet and any user can get the services from the cloud. Public Organizations helps in providing the infrastructure to execute the public cloud.

B. Private Cloud

It is used by the organizations internally and is for a single organization, anyone within the organization can access the data, services and web applications but users outside the organizations cannot access the cloud. Infrastructures of private cloud are completely managed and corporate data are fully maintained by the organization itself.

C. Hybrid Cloud

The Cloud is a combination of two or more clouds (public, private and community). Basically it is an environment in which multiple internal or external suppliers of cloud services are used. It is being used by most of the organizations (IBM and Junipers Network, 2009).

D. Community Cloud

The cloud is basically the mixture of one or more public, private or hybrid clouds, which is shared by many organization for a single cause (mostly security).Infrastructure is to be shared by several organizations within specific community with common security, compliance objectives. It is managed by third party or managed internally. Its cost is lesser then public cloud but more than private cloud.

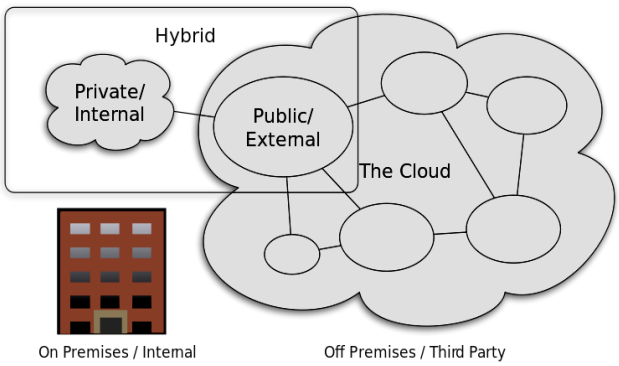

Figure 4 Types of Cloud Computing

IV. DATA SECURITY ISSUES IN THE CLOUD

A. .Privacy and Confidentiality

Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety. The cloud seeker should be assured that data hosted on the cloud will be confidential.

B .Data integrity

With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at

what point. The cloud provider should make the client aware of what particular data is hosted on the cloud, the origin and the integrity mechanisms put in place.

C. Data location and Relocation

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.. Also, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard
customers' information. Another issue is the movement of data from one location to another. Data is initially stored at appropriate location decide by the Cloud provider. However, it is often moved from one place to another. Cloud providers have contracts with each other and they use each others' resources.

D. Data Availability

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

E. Storage, Backup and Recovery

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure

V. NETWORK LEVEL SECURITY

There are different types of attacks occur in cloud computing some of which are discussed below:

A Denial of Service

When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests. In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack.

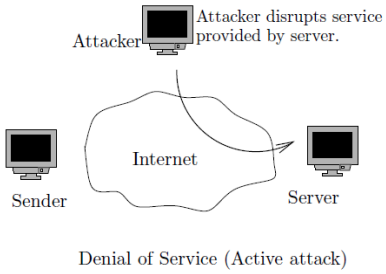

Figure 5 Denial of Service Attack

B. Man in the Middle Attack

This issue of network security that will happen if secure socket layer (SSL) is not properly configured. For example if two parties are communicating with each other and SSL is not properly installed then all the data communication between two parties could be hack by the middle party. Counter measure for this attack is SSL should properly install and it should check before communication with other authorized parties.

C. Network Sniffing

It is a more critical issue of network security in which unencrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party. Counter measure for this attack is parties should used encryption methods for securing there data.

D. Port Scanning

There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that firewall is used to secure the data from port attacks.

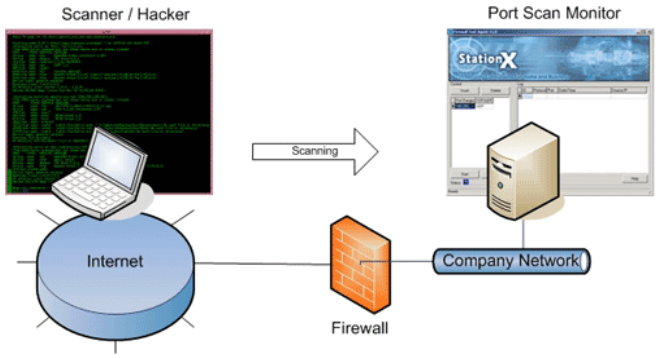

Figure 6 Port Scanning Attack

E.SQL Injection Attack

SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it. For example an

argument value of variable y or 1==1 may cause the return of full table because 1==1is always seems to be true.

F. Cross Site Scripting

It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials. For example user entered the URL in address bar and attacker redirects the user to hacker site and then he will obtain the sensitive data of the user. Cross site scripting attacks can provide the way to buffer overflows, DOS attacks and inserting spiteful software in to the web browsers for violation of user's credentials.

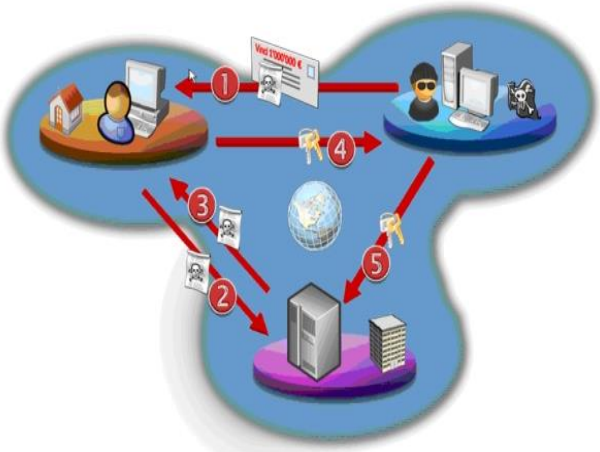

Figure 7 Cross Site Scripting

VI. ALGORITHM

RSA is widely used Public-Key algorithm. In this paper, RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who was originally known the actual data. The encryption is done by the Cloud service provider and decryption is done by the Cloud user. With out having the private key the encrypted data cannot be decrypted even the user knows the Public-Key

RSA algorithm involves in the following three steps:

- Key Generation
- Encryption
- Decryption

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two dissimilar prime numbers p and q. For security reasons, the integer's p and q should be chosen at random and should be of similar bit length.
2. Compute n = p * q
3. Calculate Ø(n) = (p-1) * (q-1)
4. Select an integer e, such that 1 < e < Ø(n) and Greatest Common Divisor (GCD) of e , Ø(n) is 1. gcd (Ø(n),e)=1
5. Calculate d as $d = e^{-1} \bmod Ø(n)$
6. d is kept as Private-Key component, so that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

Encryption

Encryption is the process of converting original plain text into cipher text.

Steps:

1. Cloud service provider should transmit the Public-Key (e, n) to the user.
2. User data is now mapped to an integer.
3. Data is encrypted and the cipher text C is $C = M^e \pmod n$.
4. This cipher text is now stored with the Cloud service provider.

Decryption:

Decryption is the process of converting the cipher text(data) to the original plain text(data).

Steps:

1. The cloud user requests the Cloud service provider for the data.
2. Cloud service provider verify's the authenticity of the user , the plain text is C.
3. The Cloud user then decrypts the data by computing $M = C^d \pmod n$.
4. After M is obtained the user can get back the original data.

VII. EXPERIMENTAL RESULTS

In this section we are taking sample data and implementing RSA algorithm over it.

Key Generation

1. Select two prime numbers , p=5 and q=7
2. Compute n = p x q =5x7=35
3. Calculate Ø(n)= (p-1)(q-1) = 24
4. Select an integer e such that 1<e<24 that is co prime to 24. We choose e=5
5. Determine d such that de=1 mod 24 and d<24. The correct value is d=5

6. Thus public key is {5,35} and Private Key is {5,35}
7. The above private key is to be secret and is known to the user only.

Encryption

1. The public key {5,35} is given by the cloud service provider to the user.
2. Let us consider an integer 3
3. Data is encrypted and the public key shared is $C= 3^5 (\text{mod } 35)=33$
4. The Data is encrypted and is stored by the cloud service provider.

Decryption

1. When user requests for the data Cloud service provider will authenticate the user and delivers then encrypted data.
2. The Cloud user decrypts the data by computing $33^5 (\text{mod } 35)= 3$
3. Once the M value is obtained user will get original data.

VIII. CONCLUSION

This paper discusses about the security aspects of three main models of cloud computing which includes SaaS, PaaS, and IaaS respectively. There are many security problem associate with cloud computing. However this paper just concentrates only on the infrastructure aspect of it. The analysis of three levels show that how SaaS, PaaS, and IaaS different from each other. Data Security has become most important issue of cloud computing security. Clients who are opting for the Services of the Cloud computing must beware of the Security concerns so that they may not be affected and lose their data. We presented an encryption algorithm RSA with the experimental values.

REFERENCES

[1] Deyan Chen , Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering 2012
[2] Peter Mell and Tim Grance, "The NIST Definition of Cloud Computing", October 7, 2009, version 15, National Institute of Standards and Technology (NIST).
[3] C.N. Höfer and G. Karagiannis, "Cloud computing services: taxonomy and comparison", Internet Serv Appl (2011)
[4] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal," A Survey on Security Issues in Cloud Computing". IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
[5] Priyanka Arora, Arun Singh and Himanshu Tyagi,"Evaluation and Comparison of Security Issues on Cloud Computing Environment", (WCSIT) ISSN: 2221-0741 Vol. 2, No. 5, p.p (179-183), 2012.
[6] Security analysis of cloud computing :(http://cloudcomputing.sys-con.com/node/1330353).
[7] Jagpal Singh,Krishnan lal and Dr.Anil kumar Shrotiya, Journal of Computer Science and Applications., ISSN 2231- 1270 Volume 4, Number 1 (2012), pp. 1-7. http://www.irphouse.com
[8] Kevin Hamlen, Murat kantarcioglu, Latifur Khan and Bhavani Thurasingham, International Journal of Information Security and Privacy, 4(2), p.p(39-51), April-June 2010.
[9] Tim Mather, Subra Kumaraswamy, and Shahed Latif. "Cloud Security and Privacy: An Enterprise Perpective on Risks and Compliance". 2009.
[10] Cloud Security Alliance. "Security Guidance for critical areas of focus in cloud computing". 2009. Ebook.